Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A method for securing software to reduce unauthorized use, the method comprising:
providing at least one hardware based authorized representative entity installed on or in a user device;
obtaining registration information corresponding to at least one user device;
generating an authentication code at least partially based on the registration information;
associating the authentication code with the software;
determining whether a current user device is authorized based on the authentication code associated with the software and registration information associated with the current user device; and
controlling access to the software based on whether the current user device is authorized.

[c2] 2. The method of claim 1 wherein the software is self activating and self authenticating in conjunction with the hardware based authorized representative located on or in the user device.

[c3] 3. The method of claim 1 wherein the software comprises data representing content selected from the group

consisting of music, video, an application program, an operating system component, a game, a movie, graphics, watermarked works, a magazine, and a book.

[c4] 4. The method of claim 1 wherein the step of obtaining registration information is at least partially performed by the at least one hardware based authorized representative entity installed on or in the user device.

[c5] 5. The method of claim 1 wherein the step of generating an authentication code is at least partially performed by the at least one hardware based authorized representative entity installed on or in the user device.

[c6] 6. The method of claim 1 wherein the step of obtaining registration information is performed by a remotely located authorized representative entity.

[c7] 7. The method of claim 1 wherein the step of generating an authentication code is performed by a remotely located authorized representative entity.

[c8] 8. The method of claim 1 wherein the steps of obtaining, generating, associating, determining, and controlling are at least partially performed by a resident hardware based authorized representative entity installed on at least one user device.

[c9] 9. The method of claim 8 wherein registration information associated with the current user device remains within a trusted network associated with the user device.

[c10] 10. The method of claim 8 wherein registration information associated with the current user device is not communicated to any third party.

[c11] 11. The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed prior to transferring the software to the current user device.

[c12] 12. The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed substantially concurrently with transferring the software to the current user device.

[c13] 13. The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed following transferring the software to the current user device.

[c14] 14. The method of claim 11 wherein the steps of obtaining, generating, and associating are performed by a re-

mote authorized representative entity.

[c15] 15. The method of claim 1 wherein the hardware based authorized representative functions are hard coded.

[c16] 16. The method of claim 1 wherein the hardware based authorized representative functions are programmable.

[c17] 17. The method of claim 1 wherein the hardware based authorized representative functions are both hard coded and programmable.

[c18] 18. The method of claim 1 wherein the hardware device is a computer chip.

[c19] 19. The method of claim 1 wherein the hardware device is integral with a CPU.

[c20] 20. The method of claim 1 wherein the hardware device is a PC card.

[c21] 21. The method of claim 1 wherein the hardware device is a microprocessor.

[c22] 22. The method of claim 1 wherein the steps of determining whether a current user device is authorized and controlling access to the software are at least partially performed by the hardware based authorized representative entity installed on or in a user device.

[c23] 23. The method of claim 1 wherein the software is electronically distributed.

[c24] 24. The method of claim 1 wherein the software is transferred to a user device from a computer readable storage medium.

[c25] 25. The method of claim 1 wherein at least one authentication code is distributed with the software.

[c26] 26. The method of claim 1 wherein the authentication code corresponds to a group of user devices.

[c27] 27. The method of claim 26 wherein the authentication code at least partially corresponds to a manufacturer of a user device.

[c28] 28. The method of claim 26 wherein the authentication code at least partially corresponds to a model of a user device.

[c29] 29. The method of claim 1 wherein the authentication code at least partially corresponds to a unique user device.

[c30] 30. The method of claim 1 wherein the steps of determining whether a current user device is authorized and controlling access to the software are performed by a re-

motely located authorized representative entity.

[c31] 31. The method of claim 1 wherein the step of controlling access to the software comprises preventing transfer of at least a portion of the software to the current user device.

[c32] 32. The method of claim 1 wherein the step of controlling access to the software comprises preventing the current user device from utilizing the software.

[c33] 33. The method of claim 1 wherein the steps of determining and controlling are at least partially performed by an authorized representative installed on a secondary user device.

[c34] 34. The method of claim 1 wherein the steps of obtaining, generating, and associating are performed by a primary user device and the steps of determining and controlling are performed by a secondary user device.

[c35] 35. The method of claim 1 further comprising encrypting the authentication code.

[c36] 36. The method of claim 1 further comprising encrypting the registration information.

[c37] 37. The method of claim 1 further comprising associating an identifier with the software to trigger authentica-

tion by an authorized representative entity.

[c38] 38. The method of claim 1 further comprising:
securing any means for generating the authentication code after generating the authentication code associated with the software.

[c39] 39. The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are at least partially performed by a hardware based authorized represenatative entity installed on or in a user device, the method further comprising:
modifying the authorized representative entity to disable subsequent generation of authentication codes associated with the software.

[c40] 40. The method of claim 1 wherein the steps of obtaining registration information, generating an authentication code, and associating the authentication code are performed by a remote authorized representative prior to distribution of the software.

[c41] 41. A method for securing software to reduce unauthorized use having an hardware based authorized representative entity installed on or in a user device, the method comprising:

determining whether the user device is authorized to access the software using the authorized representative entity; and

controlling access to the software based on whether the user device is determined to be authorized.

[c42] 42. The method of claim 41 wherein the software is self authenticating in conjunction with the authorized representative located on or in the user device.

[c43] 43. The method of claim 41 further comprising:

determining whether the user device is authorized to access the software using a remotely located authorized representative entity in combination with the authorized representative entity installed on or in the user device.

[c44] 44. The method of claim 41 wherein the hardware based authorized representative functions are hard coded.

[c45] 45. The method of claim 41 wherein the hardware based authorized representative functions are programmable.

[c46] 46. The method of claim 41 wherein the hardware based authorized representative functions are both hard coded and programmable.

[c47] 47. The method of claim 41 wherein the hardware based authorized representative entity comprises a computer

chip.

[c48] 48. The method of claim 41 wherein the hardware based authorized representative entity is integral with the CPU.

[c49] 49. The method of claim 41 wherein the hardware based authorized representative entity comprises a PC card.

[c50] 50. The method of claim 41 wherein the hardware based authorized representative entity comprises program instructions executed by a microprocessor.

[c51] 51. The method of claim 41 wherein the step of determining whether the user device is authorized comprises: comparing registration information associated with the user device to registration information associated with the software.

[c52] 52. The method of claim 51 wherein the registration information associated with the software is embedded within an authentication code.

[c53] 53. The method of claim 51 wherein the registration information associated with the software is encrypted.

[c54] 54. The method of claim 51 wherein the registration information includes hardware information.

[c55] 55. The method of claim 54 wherein the registration in-

formation includes hardware information associated with a unique user device.

[c56] 56. The method of claim 55 wherein the hardware information includes a serial number.

[c57] 57. The method of claim 54 wherein the registration information includes hardware information associated with a group of user devices.

[c58] 58. The method of claim 41 wherein the hardware based authorized representative entity is installed by a manufacturer of the user device.

[c59] 59. The method of claim 41 wherein the hardware based authorized representative entity is installed from a computer readable storage medium.

[c60] 60. The method of claim 41 wherein the hardware based authorized representative entity is downloaded to the user device.

[c61] 61. The method of claim 60 wherein the authorized representative entity is transferred to the user device from a network.

[c62] 62. The method of claim 41 wherein the step of controlling access comprises preventing the software from being transferred to a second user device.

[c63] 63. The method of claim 41 wherein the step of controlling access comprises preventing the software from being executed by the user device.

[c64] 64. The method of claim 41 wherein the step of controlling access comprises providing limited access to the software.

[c65] 65. The method of claim 41 wherein the software comprises data representing content selected from the group consisting of music, video, an application program, an operating system component, a game, a movie, graphics, watermarked works, a magazine, and a book.

[c66] 66. The method of claim 41 wherein the software comprises instructions for generating at least one authentication code at least partially based on registration information associated with the user device.

[c67] 67. The method of claim 66 wherein the software comprises instructions for encrypting the authentication code.

[c68] 68. The method of claim 41 wherein the step of determining whether the user device is authorized comprises: contacting a remote authorized representative entity if the authorized representative entity installed on or in a

user device is unable to determine whether the user device is authorized.

[c69] 69. The method of claim 41 wherein the step of determining whether the user device is authorized comprises: contacting a remote authorized representative if the authorized representative entity installed on or in a user device determines that the user device is not authorized.

[c70] 70. The method of claim 41 wherein the step of determining whether the user device is authorized comprises: obtaining registration information associated with the user device; and
comparing the registration information associated with the user device with registration information encoded in an authentication code associated with the software.

[c71] 71. The method of claim 41 further comprising:
detecting an identifier associated with the software to trigger authentication functions performed by the hardware based authorized representative entity installed on or in the user device; and
performing the steps of determining whether the user device is authorized and controlling access to the software only if the identifier is detected.

[c72] 72. The method of claim 41 further comprising:

automatically contacting a remote authorized representative based upon a triggering event to receive information.

[c73] 73. The method of claim 72 wherein the information is selected from a group consisting of updates, upgrades, patches, marketing information, promotional information, quality assurance information, network monitoring and metering information, and error and usage information.

[c74] 74. The method of claim 73 wherein the information updates the authorized representative entity installed on or in the user device.

[c75] 75. The method of claim 73 wherein the information modifies the software.

[c76] 76. The method of claim 72 wherein the triggering event is based on a user action.

[c77] 77. The method of claim 72 wherein the automatic contact with the remote authorized representitve is repeated.

[c78] 78. A method for reducing unauthorized use of software, the method comprising:
associating at least one identifier with the software cor-

responding to a request for digital rights management;
distributing the software to a user;
detecting the at least one identifier using an authorized representative entity;
associating at least one authentication code with the software;
determining whether a user device is authorized to access the software; and
controlling access to the software based on whether the user device is authorized.

[c79] 79. The method of claim 78 wherein the software is self activating and self authenticating in conjunction with a hardware based authorized representative located on or in the user device.

[c80] 80. The method of claim 78 further comprising encrypting the at least one authentication code.

[c81] 81. The method of claim 78 further comprising:
obtaining registration information associated with at least one user device; and
generating the at least one authentication code at least partially based on the registration information.

[c82] 82. The method of claim 67 further comprising encrypting the registration information.

[c83] 83. The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed before the step of distributing the software.

[c84] 84. The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed substantially concurrently with the step of distributing the software.

[c85] 85. The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed subsequent to the step of distributing the software.

[c86] 86. The method of claim 81 wherein the steps of obtaining registration information, generating the at least one authentication code, and associating the at least one authentication code are performed by an authorized representative entity installed on or in the user device.

[c87] 87. The method of claim 81 wherein the step of generating the at least one authentication code is performed by an authorized representative entity installed on or in the

user device, the method further comprising:
securing the authentication code to resist user tampering.

[c88] 88. The method of claim 87 wherein the step of securing comprises preventing the authorized representative entity installed on or in the user device from generating any more authentication codes for the software.

[c89] 89. The method of claim 87 wherein the step of securing comprises encrypting the authentication code.

[c90] 90. The method of claim 78 further comprising:
determining whether an operational authorized representative entity is available locally;
installing an authorized representative entity on or in the user device if an operational authorized representative entity is not available locally.

[c91] 91. The method of claim 90 wherein the step of installing comprises transferring the authorized representative entity to the user device from a remote authorized representative entity.

[c92] 92. The method of claim 90 wherein the step of installing comprises transferring the authorized representative entity to the user device from a computer readable storage medium.

[c93] 93. The method of claim 90 wherein the software includes an authorized representative entity and wherein the step of installing comprises transferring the authorized representative entity to the user device from the software.

[c94] 94. The method of claim 78 further comprising: determining whether an operational authorized representative entity is installed on or in the user device; and contacting a remote authorized representative entity if no operational authorized representative entity is installed on or in the user device.

[c95] 95. The method of claim 94 wherein the remote authorized representative entity performs the steps of determining whether a user device is authorized and controlling access to the software.

[c96] 96. The method of claim 78 further comprising: obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed prior to the step of distributing the software to a user.

[c97] 97. The method of claim 78 further comprising:

obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed substantially concurrently with the step of distributing the software to a user.

[c98] 98. The method of claim 78 further comprising: obtaining registration information including hardware specific information associated with a user device, wherein the steps of obtaining registration information and associating at least one authentication code are performed following the step of distributing the software to a user.

[c99] 99. The method of claim 67 wherein the step of controlling access to the software comprises preventing the software from being transferred to the user device if the user device is not authorized.